KCS Group Europe

The Unhackable Human?

26/09/2017

Pin-codes and passwords could soon become a thing of the past, as biometric technology is seeing a quiet revolution in allowing users to access and pay for facets of everyday life. But where do we draw the line - and how safe is it in a world where cyber-security is running to stand still?

Where previously passwords and PIN codes would have been required to pay in a store or gain access to an area, the rise of biometrics has meant that the human body is now able to do these things by itself. You can use a fingerprint scanner to access a phone, a retinal scanner to unlock your office or even a heartbeat tracker to get into your bank account. The goal, as with most emergent technology, is to make life easier and smoother to the point of going beyond even 'the cashless society', or similar. But there is a security-conscious motive driving this wave. Just as you cannot lose your irises or your fingerprints, these also, theoretically, cannot be stolen. It seems like a win-win for all.

Of course, technology being what it is, security through biology is far from the perfect solution that it might initially seem. Fingerprint scanners on the Apple TouchID phones were fooled just a day after use by taking an imprint of a fingerprint left on the glass. Iris scanners have been broken by using a photograph of the eye. An individual's voice recognition lock was no match for the voice of his twin brother.

There is also the problem of post-compromise rebuilding. If you lose your credit card or your PIN is lost, just cancel it and order another. It is a lot harder to get yourself a new eye, or finger if such scans fall into the wrong hands.

There is to be sure, a greater degree of complexity for the enterprising criminal to overcome in pulling off such a scam: accessing a target's body is a lot harder than accessing their wallet. However, the principle stands that even in isolated incidents; biometrics is insecure and should not be considered a savior (this is the same line of argument as applies to quantum computing a few weeks back). At the bare minimum, such technology should be the second guard in a two-factor authentication process. What it should not do is create the impression of the 'unhackable human' and throw all the security eggs in one basket.

The intention is not to disparage biometrics outright, but simply sound a warning call that any emerging technology, particularly one which has huge security implications, should be treated with equal caution as enthusiasm. And to affirm that no matter how big the advancement in technology, complacency is the biggest factor in failure.

How widespread is biometric security likely to be in our everyday lives going forward? It is difficult to say at this point, but it is hard to see a total adoption without the security, and indeed ethical, questions being resolved. People may not be comfortable giving up this level of personal information, particularly information which makes that person wholly unique. This may be one invasion of privacy too far – even in a society that is content to spread itself through devices and media to an absurd degree. Biometrics though is the ultimate expression of the form. You no longer have wearable tech, you are the tech. And in a world constantly grappling with questions of identity and safety, turning ourselves into lightning rods for compromise does not seem like the best solution.